The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

02/04/2014

SUBJECT:

Multiple Vulnerabilities in Mozilla Products Could Allow Remote Code Execution

EXECUTIVE SUMMARY:

Multiple vulnerabilities have been discovered in Mozilla Firefox, Thunderbird, and SeaMonkey applications, which could allow remote code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Thunderbird is an email client. Mozilla SeaMonkey is a cross platform Internet suite of tools ranging from a web browser to an email client. Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:

At this time, there are no known proof-of-concept exploits. Updating to the latest version of the affected software will remediate the issues.

SYSTEMS AFFECTED:

- Firefox versions prior to 27.0
- Firefox Extended Support Release (ESR) versions prior to 24.3
- Thunderbird versions prior to 24.3
- SeaMonkey versions prior to 2.24

RISK:

Government:

Large and medium government entities: **High**

Small government entities: **High**

Businesses:

Large and medium business entities: **High**

Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Thirteen vulnerabilities have been reported for various Mozilla products. Details of the vulnerabilities are as follows:

- Identified and fixed several memory safety bugs in the browser engine used in Firefox and other Mozilla-based products. Some of these bugs showed evidence of memory corruption under certain circumstances, and we presume that with enough effort at least some of these could be exploited to run arbitrary code. [MFSA 2014-01] [CVE-2014-1477] [CVE-2014-1478]
- Reported a method to bypass System Only Wrappers (SOW) by using XML Binding Language (XBL) content scopes to clone protected XUL elements. This could be used to clone anonymous nodes, making trusted XUL content web accessible. [MFSA 2014-02] [CVE-2014-1479]
- Reported that the dialog for saving downloaded files did not implement a security timeout before button selections were processed. This could be used in concert with spoofing to convince users to select a different option than intended, causing downloaded files to be potentially opened instead of only saved in some circumstances. [MFSA 2014-03] [CVE-2014-1480]
- Reported issue with image decoding in RasterImage caused by continued use of discarded images. This could allow for the writing to unowned memory and a potentially exploitable crash. [MFSA 2014-04] [CVE-2014-1482]
- Reported an information leak where document.caretPositionFromPoint and document.elementFromPoint functions could be used on a cross-origin iframe to gain information on the iframe's DOM and other attributes through a timing attack, violating same-origin policy. [MFSA 2014-05] [CVE-2014-1483]
- Profile path leaks to Android system log - Reported that Firefox for Android profile paths leak to the Android system log. When running on Android 4.2 or earlier, other applications are able to read these log files, leading to information disclosure from the user's profile directory. This issue was also independently reported by Mozilla developer Richard Newman. [MFSA 2014-06] [CVE-2014-1484]
- Reported an issue where the implementation of Content Security Policy (CSP) is not in compliance with the specification. XSLT stylesheets must be subject to script-src directives but Mozilla's implementation of CSP treats them as styles. This could lead to unexpected script execution if the style-src directives were less restrictive than those for scripts. [MFSA 2014-07] [CVE-2014-1485]
- Reported a use-after-free during image processing from sites with specific content types in concert with the imgRequestProxy function. This causes a potentially exploitable crash. [MFSA 2014-08] [CVE-2014-1486]
- Reported a cross-origin information leak through web workers' error messages. This violates same-origin policy and the leaked information could potentially be used to gather authentication tokens and other data from third-party websites. [MFSA 2014-09] [CVE-2014-1487]
- Reported flaw that once users have viewed the default Firefox start page (about:home), subsequent pages they navigate to in that same tab could use script to activate the buttons that were on the about:home page. Most of these simply open Firefox dialogs such as Settings or History, which might alarm users. In some cases a malicious page could trigger session restore and cause data loss if the current tabs are replaced by a previously stored set. [MFSA 2014-10] [CVE-2014-1489]
- Reported a crash when terminating a web worker running asm.js code after passing an object between threads. This crash is potentially exploitable. [MFSA 2014-11] [CVE-2014-1488]
- Reported issues with ticket handling in the Network Security Services (NSS) libraries. These have been addressed in the NSS 3.15.4 release, shipping on affected platforms. [MFSA 2014-12] [CVE-2014-1490] [CVE-2014-1491]
- Reported an inconsistency with the different JavaScript engines in how JavaScript native getters on window objects are handled by these engines. This inconsistency can lead to different behaviors in JavaScript code, allowing for a potential security issue with window handling by bypassing of some security checks. [MFSA 2014-13] [CVE-2014-1481]

Successful exploitation could result in an attacker gaining the same privileges as the affected application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

RECOMMENDATIONS:

The following actions should be taken:

- Update vulnerable Mozilla products immediately after appropriate testing by following the steps outlined by Google.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Do not open email attachments or click on URLs from unknown or untrusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Mozilla:

http://www.mozilla.org/security/announce/2014/mfsa2014-01.html

http://www.mozilla.org/security/announce/2014/mfsa2014-02.html

http://www.mozilla.org/security/announce/2014/mfsa2014-03.html

http://www.mozilla.org/security/announce/2014/mfsa2014-04.html

http://www.mozilla.org/security/announce/2014/mfsa2014-05.html

http://www.mozilla.org/security/announce/2014/mfsa2014-06.html

http://www.mozilla.org/security/announce/2014/mfsa2014-07.html

http://www.mozilla.org/security/announce/2014/mfsa2014-08.html

http://www.mozilla.org/security/announce/2014/mfsa2014-09.html

http://www.mozilla.org/security/announce/2014/mfsa2014-10.html

http://www.mozilla.org/security/announce/2014/mfsa2014-11.html

http://www.mozilla.org/security/announce/2014/mfsa2014-12.html

http://www.mozilla.org/security/announce/2014/mfsa2014-13.html

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1477

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1478

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1479

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1480

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1481

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1482

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1483

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1484

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1485

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1486

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1487

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1488

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1489

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1490

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1491

SecurityFocus:

http://www.securityfocus.com/bid/65316

http://www.securityfocus.com/bid/65317

http://www.securityfocus.com/bid/65320

http://www.securityfocus.com/bid/65321

http://www.securityfocus.com/bid/65322

http://www.securityfocus.com/bid/65323

http://www.securityfocus.com/bid/65324

http://www.securityfocus.com/bid/65326

http://www.securityfocus.com/bid/65328

http://www.securityfocus.com/bid/65329

http://www.securityfocus.com/bid/65330

http://www.securityfocus.com/bid/65331

http://www.securityfocus.com/bid/65332

http://www.securityfocus.com/bid/65334

http://www.securityfocus.com/bid/65335